National Energy Research Scientific Computing Center
A DOE Office of Science User Facility
at Lawrence Berkeley National Laboratory

NERSC Computer Use Policies Form

This is a list of general computer use policies and security rules that apply to all users of NERSC computers or networks. Principal Investigators are responsible for implementing these policies and procedures in their organization and ensuring that users fulfill their responsibilities. **NERSC must have a signed copy of this form on file for every user.** If you are reading this form online, please print out a copy; sign and return to NERSC (see fax and U.S. address below).

Computer Use	Computers, software, and communications systems provided by NERSC are to be used only for DOE-sponsored work (as determined by the DOE Program Monitor). **Use of NERSC resources to store, manipulate, or remotely access any national security information is prohibited. This includes, but is not limited to, classified information, unclassified controlled nuclear information (UCNI), naval nuclear propulsion information (NNPI), the design or development of nuclear, biological, or chemical weapons or of any weapons of mass destruction.** The use of NERSC resources for personal or non-work-related activity is also prohibited. NERSC systems are provided to our users without any warranty. NERSC will not be held liable in the event of any system failure or loss of data.
Foreign National Access	Principal Investigators are required to inform NERSC if any of their users are foreign nationals and from what country. **Access to NERSC computers is denied to a foreign national not lawfully admitted for permanent residence in the United States from countries on the Department of Commerce "Computer Tier 4" list.** As of January 10, 2001, these countries are Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria. Additionally, no work may be performed on NERSC computers on behalf of foreign nationals from these countries. Access to NERSC computers by foreign nationals not lawfully admitted for permanent residence in the United States that would involve a release of U.S.- origin software or technology will be reviewed on a case-by-case basis.
Data Retention	When a user account is deleted, all permanent files (in home directories and NERSC mass storage systems) are assigned to the PI, who is responsible for deleting unneeded files.
User Accountability	Users are accountable for their actions and may be held accountable to applicable administrative or legal sanctions.

Passwords and Usernames	A user identifier known as a username and password are required of all users. Passwords must be changed at least every six months. Passwords must contain at least eight nonblank characters, must contain a combination of upper and lowercase letters, numbers, and at least one special character within the first seven positions, must contain a nonnumeric letter or symbol in the first and last positions, must not contain the user login name, must not include common words from a dictionary, must not contain commonly used proper names, including the name of any fictional character or place, nust not include the user's or a close friend's or a relative's name or any information about him or her that the user believes could be readily learned or guessed. The complete password policy is at http://www.nersc.gov/nusers/accounts/password.php. Passwords must not be shared with any other person. The password must be changed as soon as possible after an unacceptable exposure or suspected compromise.
Unauthorized Access	Users are not to attempt to receive unintended messages or access information by some unauthorized means, such as imitating another system, impersonating another user or other person, misuse of legal user credentials (usernames, passwords, etc.), or by causing some system component to function incorrectly.
Software Use	All software used on NERSC computers must be appropriately acquired and used according to the appropriate licensing. Possession or use of illegally copied software is prohibited. Likewise, users shall not copy, store or transfer copyrighted software or data, except as permitted by the owner of the copyright.
Altering Authorized Access	Users are prohibited from changing or circumventing access controls to allow themselves or others to perform actions outside their authorized privileges.
Reconstruction of Information or Software	Users are not allowed to reconstruct or recreate information or software for which they are not authorized.
Data Modification or Destruction	Users are prohibited from taking unauthorized actions to intentionally modify or delete information or programs.
Malicious Software	Users must not intentionally introduce or use malicious software such as computer viruses, Trojan horses, or worms.
Denial of Service Actions	Users may not deliberately interfere with other users accessing system resources.
Notification	Users must notify NERSC immediately when they become aware that any of the accounts used to access NERSC has been compromised.
Account Usage	Users are not allowed to share their accounts with others.

NERSC personnel and users are required to address, safeguard against and report misuse, abuse and criminal activities. Misuse of NERSC resources can lead to temporary or permanent disabling of accounts, loss of DOE allocations, and administrative or legal actions.

Sign and return to NERSC:

by FAX to (+1) 510-486-4248
OR by Postal Service to:
NERSC Account Support / Lawrence Berkeley National Laboratory
One Cyclotron Rd.
MS 50A1148
Berkeley, CA 94720

I have read the NERSC Policies and Procedures and understand my responsibilities in the use of NERSC resources.

Signature:

Print Name:

Citizenship:

Organization:

Email Address:

Work Phone Number:

Principal Investigator:

Date: